Kay Bailey Hutchison, Chairman
Bill Hughes, Staff Director

347 Russell Senate Office Building
Washington, DC 20510
202-224-2946
http://rpc.senate.gov

SENATE REPUBLICAN POLICY COMMITTEE

January 23, 2008

FISA Modernization and Carrier Liability

Executive Summary

- In a 13 to 2 vote, the Senate Select Committee on Intelligence (SSCI) reported S. 2248, the FISA Amendments Act of 2007, which is designed to safeguard vital intelligence-gathering while protecting civil liberties.

- The assistance of private telecommunications carriers is essential to carrying out the intelligence-gathering contemplated in FISA. S. 2248 provides prospective immunity to those carriers whose cooperation will be needed in the future.

- S. 2248 also provides immunity to private carriers from civil suits arising out of their alleged cooperation with the National Security Agency's "Terrorist Surveillance Program" (TSP) between September 11, 2001 and January 17, 2007.

- Any assistance provided to the TSP was in response to written requests or directives from senior officials which stated that the assistance was required in connection with intelligence activity that was necessary to detect or prevent possible terrorist attacks; had been authorized by the President; and had been determined to be legal.

- The carriers nonetheless face more than 40 lawsuits by parties seeking hundreds of billions of dollars in damages.

- For reasons of fairness and national security, the civil litigation against private carriers should come to an immediate and final end.

- Alternatives to immunity would not alleviate the inequities and dangers of continuing civil litigation.

  The proposal for FISA Court review of the carriers' good faith cooperation with the government would be onerous and impracticable. The carriers had little choice but to trust the government and put the national interest above their own.

Introduction

The Terrorist Surveillance Program

After the attacks of September 11, 2001, the President instituted what came to be known as the Terrorist Surveillance Program (TSP). The TSP provided a way to intercept the communications of foreign terror suspects abroad in order to detect or prevent terrorist attacks, or activities in preparation for a terrorist attack.

Though the details of the TSP remain highly classified, its existence was revealed by the *New York Times* in December 2005. It was reported that the TSP relied on the cooperation of telecommunications service providers in a variety of ways. But according to a recent report of the Senate Select Committee on Intelligence (SSCI), the carriers acted in each case in response to "written requests or directives […] to obtain their assistance with communications intelligence activities that had been authorized by the President." The SSCI has reviewed the pertinent correspondence, and notes that:

> The letters were provided to electronic service providers at regular intervals. All of the letters stated that the activities had been authorized by the President. All of the letters also stated that the activities had been determined to be lawful by the Attorney General, except for one letter that […] stated that the activities had been determined to be lawful by the Counsel to the President.[1]

On January 17, 2007, the Attorney General (AG) announced that what had been known as the TSP would henceforth be conducted pursuant to procedures approved by the Foreign Intelligence Surveillance (FISA) Court and subject to its review. However, a subsequent ruling of the FISA Court imposed additional administrative requirements that, according to the Director of National Intelligence (DNI), crippled the Intelligence Community's ability to conduct surveillance of foreign terror suspects. This led to passage of the emergency, 180-day "FISA fix" in the Protect America Act (PAA; P.L. 110-55), which sunsets on February 1, 2008.

Litigation related to the TSP

The revelation of the TSP's existence triggered a wave of complex litigation at the federal and state level aimed both at private carriers and at the government. More than 40 federal lawsuits allege the service providers assisted the government by providing information about the communications of persons within the United States. Collectively, they seek hundreds of billions of dollars in damages. In addition, a number of state regulatory proceedings have been initiated against private carriers on the basis of alleged violations of state privacy rights. Suits have also been brought against the government and against government officials alleging statutory and constitutional violations.

This paper examines the three main alternative mechanisms that have been proposed to deal with the problematic issues of carrier liability arising out of the litigation related to the TSP from

[1] Report of the Senate Select Committee on Intelligence to accompany S. 2248, S. Rept. 110-209.

September 11, 2001 to January 17, 2007[2]: immunity, indemnification, and substitution. At its fullest extent, immunity could theoretically provide for dismissal-on-petition of court claims against both private carriers and the government in both civil and criminal proceedings. Indemnification would compensate private carriers for money damages incurred as a result of their cooperation with the government's anti-terrorism efforts. Substitution would substitute the government for the carriers as parties in proceedings targeted at the latter. This paper also examines efforts to require judicial review of the carriers' claims of good faith belief that their cooperation with the TSP had been determined to be legal.

The most serious problems engendered by the continuation of TSP-related litigation against the carriers, whether as parties-defendant or defendants only for purposes of discovery, can only be resolved through a final and complete end to the litigation. It is unfair to leave carriers exposed to litigation risk and onerous discovery requests for actions that they took in the national interest, and at considerable risk to their own. Moreover, every day that the litigation continues leaves vital sources and methods of the Intelligence Community vulnerable to discovery requests; this is especially true given the indeterminate and unpredictable balancing tests that judges use to assess claims of state-secrets privilege. Equally serious are the dangers to the carriers themselves. Some carriers have made it known that if they are not given immunity, they may refuse to cooperate with the government in any area of surveillance activity (including law enforcement) except under strict compulsion. Continued litigation might even put at risk the physical safety of the carriers' employees – especially those who work abroad – as the identities of those who helped the government in the fight against terrorism are revealed.

Main Alternatives for Carrier Liability Protection

Immunity

During the 2007 deliberations on FISA modernization, the administration argued vigorously for blanket retroactive immunity for government officials as well as private carriers in both civil and criminal proceedings. The SSCI determined that such immunity was broader than necessary; while several alternatives were too narrow. It developed a compromise structure that provides limited immunity to private carriers in civil suits arising from the TSP. Under the SSCI bill, immunity does not extend to government officials or to any criminal proceedings that may arise in the future out of the TSP.

The SSCI bill's immunity mechanism, which was affirmed by a committee vote of 12 to 3, provides for dismissal of civil actions brought in federal or state courts seeking monetary or other relief against private carriers or their employees for providing assistance to the government upon a certification by the AG. To be sufficient, the certification must state either that the alleged assistance was not provided, or that it was provided in connection with intelligence activity that was authorized by the President between September 11, 2001 and January 17, 2007; that the intelligence activity was designed to detect or prevent a terrorist attack (or preparations

[2] Potential liability arising out of cooperation provided by carriers in conformity with FISA as amended by the PAA or the FISA Amendments Act is covered by immunity provisions similar to those contained in the original FISA of 1978, and are not at issue here. Only protection from claims arising out of the TSP will be discussed in this paper.

for one) against the United States; and that assistance was provided upon a written request or directive from the AG or head (or deputy head) of an element of the intelligence community stating that the activity had been authorized by the President and had been determined to be lawful. Any assistance provided by the carrier above and beyond what was requested would not be covered by the SSCI's immunity mechanism. The SSCI bill also covers a handful of state regulatory investigations that have arisen (or may arise) out of cooperation with the TSP. Under the bill, all such proceedings against private carriers are preempted.

Indemnification

Under indemnification, the United States would compensate private carriers for any liability incurred as a result of TSP-related litigation. This proposal has failed to gain much support for several reasons. Even under indemnification there would be considerable litigation costs for private carriers. Because of the government's state secrets privilege, they would in most cases be barred from providing the evidence needed to substantiate their defenses. Indemnification would incentivize trial lawyers seeking "deep pockets" to structure complex and costly litigation that promises a high possible return even where the probability of succeeding on the merits is low. Indemnification would presumably not compensate carriers in the case of a pre-judgment settlement, but they might settle anyway, at enormous cost, to protect vital business interests. Finally, the danger to national security from revelation of sources and methods, and to the carriers and their employees from revelation of information about a carrier's assistance to the government, might vastly outweigh the benefits to plaintiffs.

Substitution

Another proposed mechanism for carrier liability protection is substitution, in which the government would be substituted for private carriers in civil suits against them.

A straightforward substitution mechanism is presented in S. 2402, the Foreign Intelligence Surveillance Substitution Act. The bill has the same scope of coverage as the immunity provision of S. 2248 in terms of the covered actions and the elements of the required AG certification (including the requirement that the carrier have acted in response to a written request or directive stating that the intelligence activity had been authorized by the President and had been determined to be lawful). Like S. 2248, it also protects carriers only to the extent that their assistance to the government does not exceed what was requested. The essential difference between immunity and substitution is that, instead of dismissing the claim upon a sufficient AG certification for all purposes, the court would dismiss the claim *as to the defendant private carrier*, and substitute in its place the United States.

Under S. 2402, carriers would still be subject to "third-party discovery requests" in any suits that continue against the government as substituted defendant.[3] S. 2402 also provides that the

[3] In the case of deposition requests, S. 2402 provides that any private carrier relieved by substitution would still be subject to the deposition request and its answers and admissions deemed binding upon the government.

government, as substituted defendant, would generally be allowed only those statutory defenses available to the carrier. This ensures that the government would not be able to assert, for example, a defense based on expiration of any statute of limitations available to it by statute. On the other hand, evidentiary *privileges* (such as state secrets privilege) would still be available to the government, as in a normal suit.

It has been argued that this proposal is preferable to indemnification because it would relieve the private carriers of the burden of litigating claims more properly brought against the government, but for whom the carriers would not have provided the challenged assistance. But the continued discovery against the carriers under S. 2402 would engender many of the dangers of providing them no relief at all.

It has been argued that substitution is preferable to immunity because the government must be held accountable for the TSP. On the other hand, the legality of the TSP is already being tested in the many cases that have been brought against the government itself.

Court review of carriers' good faith cooperation with TSP

Near the end of the first session of this Congress, Senator Feinstein presented an amendment (S.A. 3858) that provides immunity similar to that contemplated in the SSCI bill, except that the immunity is only available if, after review, the FISA Court determines that (i) the request or directive relied on by the carrier in furnishing the assistance complied with the 18 U.S.C. § 2511(2)(a)(ii)(B)[4] requirements for similar requests in the criminal law enforcement context; (ii) the assistance was "undertaken in good faith […] pursuant to a demonstrable reason to believe that compliance […] was permitted by law; or (iii) the provider did not provide the alleged assistance."

The first of these elements, compliance with § 2511, raises the possibility the immunity will be denied on the basis of a technical requirement which neither the carriers nor the government could have predicted they would one day be subject to. Intelligence-gathering in wartime (as opposed to the criminal law enforcement context of § 2511) has always been conducted pursuant to core Article II powers of the President. In any event, the letters appear to have complied substantially with the requirements of § 2511: they were in writing; they came from the AG or head or deputy head of an element of the Intelligence Community; they stated that the TSP had been duly authorized and had been determined to be legal; and they presumably set forth with specificity the nature and scope of the assistance requested.

The most serious problem with the Feinstein amendment is the requirement that the FISA Court determine in each case whether the assistance was undertaken in good faith pursuant to a

[4] 18 U.S.C. § 2511(2)(a)(ii)(B) authorizes persons to provide the government certain assistance related to electronic communications without a court order only upon "a certification in writing by [certain persons] or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required."

"demonstrable reason to believe" that the assistance was legal. But any review, by any federal court, of the carriers' good faith reliance on the government's assurances would in effect require that each carrier produce evidence of a contemporaneous (presumably written) legal opinion on the TSP itself. But carriers could not have predicted that they would one day be subject to this requirement, and in any case they almost certainly would not have been given enough information about the highly secret TSP to assess its legality. Indeed, those employees who were actually contacted by the government were almost certainly "read into" a security "compartment" and specifically prohibited from discussing the matter with anybody. In sum, they had little choice but to put the national interest above their own and rely on the government's assurances that the program had been determined to be legal.[5]

The Feinstein amendment is also impracticable with the FISA Court as currently constituted. The amendment would require that the FISA Court make its determinations *en banc* (i.e., all the judges sitting together) and that plaintiffs and defendants be allowed to appear before it. But the federal judges who make up the FISA Court sit in districts across the country. By design, they are seldom, if ever, in the Nation's Capital or anywhere else at the same time. They take turns rotating through Washington, DC to sign such orders as may be needed under FISA, in a special room designated for the purpose at the Department of Justice. The FISA Court has no statutory procedures or administrative capacity to hear witnesses, least of all *en banc*.

Conclusion

Civil liability protection for private carriers who allegedly assisted the government's Terrorist Surveillance Program at considerable risk to themselves is not only fair, but also necessary to ensure both their continued assistance and that our sources and methods are safeguarded. The fair and prudent thing to do is to bring an immediate and final end to the ongoing drama of civil litigation against companies accused of nothing more than helping to protect Americans at home during a period of unprecedented danger.

[5] Much as one would on a "no action letter" from a regulatory agency such as the Securities and Exchange Commission.